Coronavirus e smart working: l’impatto sulla cyber security

Le misure adottate per smorzare la diffusione della pandemia Covid-19 hanno mutato, senza ombra di dubbio, non solo il nostro modo di vivere ma anche quello di lavorare.

Il ricorso allo *smart working*, imposto dall’emergenza come unica soluzione lavorativa in grado di garantire distanziamento sociale e nel contempo la continuità operativa, ne rappresenta un esempio lampante.

Sfortunatamente però questo passaggio – avvenuto senza una corretta pianificazione e, talvolta, in modo estemporaneo – ha fornito **un *assist* al *cyber crime*** che, sfruttando le vulnerabilità dei nuovi strumenti e i timori correlati al disagio e allo stato di crisi, ha colto l’occasione per capitalizzare i propri profitti illeciti con campagne di *phishing*, *malspam* e attacchi informatici.
Tale fenomeno, pur attenuatosi durante il periodo estivo, dopo aver registrato nella prima metà del 2020 un certo incremento (tra febbraio e giugno sono stati registrati 119 attacchi gravi a tema Covid-19 pari al 14% degli attacchi complessivamente noti, a fronte di un incremento generale del +7% – fonte rapporto Clusit 2020), ha ripreso vigore in autunno con le stesse modalità e continuando a far leva sulle paure connesse alla pandemia.

Purtroppo, all’aumento esponenziale dell’impiego di piattaforme tecnologiche di videoconferenze e desktop remoto non sono seguite delle azioni utili a colmare quelle lacune già in essere che hanno finito con l’impattare negativamente anche sulla sicurezza informatica: ogni organizzazione che estenda il perimetro e gli ambiti di azione della propria

infrastruttura di rete, aumentando, di fatto, la propria potenziale **superficie di attacco**, deve assolutamente continuare a garantire un livello di protezione paragonabile a quello che si dovrebbe garantire per una rete aziendale estesa localmente e non in modo distribuito. Senza continuare a commettere l'errore di ritenere che lo *smart working*, delocalizzando il luogo di lavoro, possa deresponsabilizzare le aziende e liberarle da questo impegno, in questo contesto è, invece, necessario ragionare su quali siano gli aspetti e i rischi che possono impattare sulla sicurezza informatica, fattori da non sottovalutare e da prendere seriamente in considerazione.

Oggi non è più ammesso continuare a sbagliare, ma bisogna mettere in campo tutte le misure necessarie per uno *smart working* sicuro individuando e attuando soluzioni adeguate.

I requisiti di sicurezza

Occorre certamente cercare di attenuare il più possibile l'esposizione al rischio cyber con adeguate strategie strutturali secondo le raccomandazioni del NIST e dello standard ISO/IEC, proteggendo *server*, *client* e accessi remoti intrinsecamente suscettibili a una varietà di attacchi, di tipo MitM, DDoS e *brute force*, che minano principalmente la **riservatezza** e l'**integrità** delle comunicazioni e la disponibilità degli accessi alle risorse.

I dispositivi per il lavoro agile

La valutazione su quali – e come – usare i dispositivi personali per l'attività lavorativa *smart* secondo il paradigma **BYOD** (*Bring Your Own Device*) gioca un ruolo importante nella determinazione del fattore di rischio. Infatti, l'utilizzo sul dispositivo lavorativo della posta elettronica privata o di social network personali può esporre a seri problemi di sicurezza e privacy non soltanto il dipendente, quanto la stessa azienda per la quale lavora.

Sarebbe, pertanto, auspicabile che l'attività lavorativa in modalità agile avvenisse esclusivamente attraverso dispositivi forniti dall'azienda secondo una politica che ne impedisca un utilizzo diverso da quello lavorativo e che contestualmente salvaguardi da possibili incidenti di sicurezza e/o violazioni della privacy, soprattutto in considerazione del fatto che le reti e i sistemi usati a domicilio dai dipendenti per lavoro rappresentano, essi stessi, potenziali crepe per la sicurezza informatica aziendale.
Basti ricordare come *router* domestici, reti VPN e piattaforme per video conferenze siano già stati presi di mira sfruttando ogni tipo di vulnerabilità.

Smart working – gli strumenti di protezione

Le modalità con cui proteggere i dispostivi di lavoro, il perimetro esteso delle infrastrutture di rete e le connessioni remote vanno assolutamente integrate, senza discrezionalità, anche con un serio processo di accrescimento tra gli utenti della consapevolezza di tutti i rischi correlati.

Per innalzare il livello di protezione dell'organizzazione, risultano quanto mai indispensabili iniziative di sensibilizzazione sui vari aspetti della sicurezza delle informazioni rivolte a tutto il personale, di ogni ordine e grado. Un adeguato programma di *security awareness* modulato tramite formazione a distanza, newsletter o intranet aziendali può fornire delle competenze basilari e opportune linee guida per la prevenzione e le regole di comportamento utili per evitare danni in termini di privacy, sicurezza, *business continuity* e reputazione.

Per la protezione perimetrale estesa e le connessioni alle reti aziendali da remoto è poi fondamentale utilizzare **protocolli di comunicazione sicuri** basati su adeguate connessioni VPN e verificare che tutti dispositivi di

protezione della rete siano, in generale, costantemente aggiornati e adeguatamente hardenizzati.

Allo scopo di confinare le informazioni all'interno di un perimetro esteso e protetto, garantendo al contempo la continuità dei servizi, andrebbero applicate:

- tecniche per la gestione delle risorse in ambienti virtualizzati;
- attività di *management* e controllo allo scopo di identificare vulnerabilità su *server, gateway, firewall* e *client*, legate all'estensione del perimetro della struttura IT aziendale;
- soluzioni di *alerting* e di backup scalabili in base alle esigenze e criticità;
- misure per attenuare il rischio di attacchi volumetrici, evitando che un'indisponibilità di una risorsa e/o di un sistema determini un blocco o un rallentamento significativo dell'intera attività lavorativa.

Infine, per la protezione dei dispostivi *client* risulterebbero utili:

- una dotazione di sistemi antivirus aggiornati periodicamente;
- adeguate configurazioni *hardening* (chiusura di porte I/O, disabilitazione di privilegi amministrativi, disinstallazione di programmi non necessari, limitazione e controllo navigazione, posta elettronica e accessi) mirate a minimizzare l'impatto di possibili attacchi informatici che potrebbero sfruttare determinate vulnerabilità degli stessi dispositivi;
- sistemi di cifratura del *file system*, al fine di prevenire la perdita di dati sensibili in caso di furti o smarrimenti accidentali.

In conclusione

Le varie modalità di “lavoro agile” saranno, con molta probabilità, destinate ad essere soluzioni utilizzate dalle aziende e organizzazioni anche nel post emergenza, soprattutto per i vantaggi concernenti la produttività, la flessibilità e il risparmio in termini di costi e spazi. Occorre pertanto implementarle, gestirle e mantenerle in modo corretto e sicuro.

È importante dunque adottare misure per mitigare gli impatti negativi che attacchi informatici ripetuti possono avere sull’operatività di settori produttivi, essenziali e istituzionali, migliorando la prevenzione e il controllo e collaborando sinergicamente affinché – anche per la *cyber security* – l’attuale crisi possa rappresentare davvero un’eccezionale opportunità di crescita e cambiamento.

Riferimenti

Articolo a cura di **Salvatore Lombardo**

Salvatore Lombardo è laureato in Ingegneria Elettronica orientamento Telematico. Ha frequentato un Master in Information and Communication Technologies – Internet Software Engineering.

Da oltre dieci anni svolge l’attività di funzionario informatico presso la Pubblica Amministrazione, curando in particolare la sicurezza informatica e l’amministrazione di rete.

In qualità di esperto ICT, iscritto all’albo dei docenti della ex Scuola Superiore dell’Amministrazione dell’Interno, ha tenuto vari corsi di formazione e aggiornamento per il personale.

È autore del libro La Gestione della Cyber Security nella

Pubblica Amministrazione.

https://www.ictsecuritymagazine.com/articoli/coronavirus-e-smart-working-limpatto-sulla-cyber-security/